
THE CHAMELEON ATTACK: MANIPULATING CONTENT DISPLAY IN ONLINE SOCIAL MEDIA

A PREPRINT

Aviad Elyashar, Sagi Uziel, Abigail Paradise, and Rami Puzis

Telekom Innovation Laboratories and Department of Software and Information Systems Engineering,
Ben-Gurion University of the Negev, Beer-Sheva, Israel
{aviade, sagiuz, abigailp}@post.bgu.ac.il, puzis@bgu.ac.il

January 17, 2020

ABSTRACT

Online social networks (OSNs) are ubiquitous attracting millions of users all over the world. Being a popular communication media OSNs are exploited in a variety of cyber attacks. In this article, we discuss the *Chameleon* attack technique, a new type of OSN-based trickery where malicious posts and profiles change the way they are displayed to OSN users to conceal themselves before the attack or avoid detection. Using this technique, adversaries can, for example, avoid censorship by concealing true content when it is about to be inspected; acquire social capital to promote new content while piggybacking a trending one; cause embarrassment and serious reputation damage by tricking a victim to like, retweet, or comment a message that he wouldn't normally do without any indication for the trickery within the OSN. An experiment performed with closed Facebook groups of sports fans shows that (1) *Chameleon* pages can pass by the moderation filters by changing the way their posts are displayed and (2) moderators do not distinguish between regular and *Chameleon* pages. We list the OSN weaknesses that facilitate the *Chameleon* attack and propose a set of mitigation guidelines.

Keywords Chameleon Attack, Online Social Networks

1 Introduction

The following scenario is not a conventional introduction. Rather, it's a brief example to stress the importance and potential impact of the disclosed weakness, unless the countermeasures described in this article are applied.

Example 1 (A teaser) *Imagine a controversial Facebook post shared by a friend of yours. You have a lot to say about the post, but you would rather discuss it in person to avoid unnecessary attention online. A few days later when you talk with your friend about the shared post, the friend does not understand what you're referring to. Both of you scan through his/her timeline and nothing looks like that post. The next day you open Facebook and discover that in the last six months you have joined three Facebook groups of Satanists; you actively posted on a page supporting an extreme political group (although your posts are not directly related to the topics discussed there), and you liked several websites leading to video clips with child abuse. A terrible situation that could hurt your good name especially if you are a respected government employee!*

At the time of submission of this article, the nightmare described in Example 1 is still possible in major online social networks (OSNs) (see Section 4) due to a conceptual design flaw.

Today, OSNs are an integral part of our lives [1]. They are powerful tools for disseminating, sharing and consuming information, opinions, and news [2]; and for expanding connections [3], etc. However, OSNs are also constantly abused by cybercriminals who exploit them for malicious purposes including spam and malware distribution [4], harvesting personal information [5], infiltration [6], and spreading misinformation [7]. Bots, fake profiles, and fake information are all well-known scourges being tackled by OSN providers, academic researchers, and organizations around the world

with various levels of success. It is extremely important to constantly maintain the content of social platforms and service-wise, in order to limit abuse as much as possible.

In order to provide the best possible service to their users, OSNs allow users to edit or delete published content [8], edit user profiles, and update previews of linked resources, etc. These features are important in order to keep social content up to date, to correct grammatical or factual errors in published content, and eliminate abusive content. Unfortunately, they also open an opportunity for a scam where OSN users are tricked into engaging with seemingly appealing content that is later modified. This type of scam is trivial to execute and is out of the scope of this article.

Facebook partially mitigates the problem of modifications made to posts after their publication by displaying an indication that a post was edited. Other OSNs, such as Twitter or Instagram, do not allow published posts to be edited. Nevertheless, the major OSNs (Facebook, Twitter, and LinkedIn) allow publishing redirect links, and they support link preview updates. This allows changing the way a post is displayed without any indication that the target content of the URLs has been changed.

In this article, we present a novel type of OSN attack termed the *Chameleon* attack, where the content (or the way it is displayed) is modified over time in order to create social traction before executing the attack (see Section 3). We discuss the OSN misuse cases stemming from this attack and their potential impacts in Section 3.3. We review the susceptibility of seven major OSN platforms to the *Chameleon* attack in Section 4 and present the results of an intrusion into closed Facebook groups facilitated by it in Section 5. A set of suggested countermeasures that should be applied to reduce the impact of similar attacks in the future is suggested in Section 4.3.

The contribution of this study is three-fold:

- We present a new OSN attack termed the *Chameleon* attack including an end-to-end demonstration on major OSNs (Facebook, Twitter, and LinkedIn).
- We present a social experiment on Facebook showing that chameleons facilitate infiltration into closed communities.
- We discuss multiple misuse cases and mitigation methods from which we derive a recommended course of action to OSNs.

2 Background on redirection and link preview

Redirection Redirection is a common practice on the Web that helps Internet users to find relocated resources, to use multiple aliases for the same resource, and to shorten long and cumbersome URLs. As a case in point, the use of URL shortening services is very common within OSNs.

There are two types of redirect links: server, and client redirects. In case of a server-side redirect, the server returns the HTTP status code 301 (redirect) with a new URL. Major OSNs follow server-side redirects up to the final destination in order to provide their users with a preview of the linked Web resource. In the case of a client-side redirect, the navigation process is carried out by a JavaScript command executed in the client’s browser. Since the OSNs do not render the Web pages they do not follow the client redirects up to the final destination.

Short links and brand management There are many link redirection services across the Web that use 301 server redirects for brand management, URL shortening, click counts and various website access statistics. Some of these services that focus on brand management, such as `rebrandly.com`, allow their clients to change the target URL while maintaining the aliases. Some services, such as `bitly.com`, require a premium subscription to change the target URL. The ability to change the target URL without changing the short alias is important when businesses restructure their websites or move them to a different web host. Yet, as will be discussed in Section 3, this feature may be exploited to facilitate the *Chameleon* attack.

DNS updates DNS is used to resolve the IP address of a server given a domain name. The owner of the domain name may designate any target IP address for his/her domain and change it at will. The update process may take up to 24 hours to propagate. Rapid DNS update queries, known as Fast Flux, are used by adversaries to launch spam and phishing campaigns. Race conditions due to the propagation of DNS updates cause a domain name to be associated with multiple, constantly changing IP addresses at the same time.

Link previews Generating and displaying link previews is an important OSN feature that streamlines the social interaction within the OSN. It allows the users to quickly get a first impression of a post or a profile without extra clicks. Based on the met-tags of the target page, the link preview, usually includes a title, a thumbnail, and a short description of the resource targeted by the URL [9].

When shortened URLs or other server-side redirects are used, the OSN follows the redirection path to generate a preview of the final destination. These previews are cached due to performance considerations. The major OSNs update the link previews upon request (see Section 4.2 for details). In the case of client-redirect, some OSNs (e.g. Twitter) use the meta-tags of the first HTML page in the redirect chain. Other, e.g. Facebook, follow the client redirect up to the final destination.

3 The Chameleon Attack

The *Chameleon* attack takes advantage of link previews and redirected links to modify the way that published content is displayed within the OSN without any indication for the modifications made. As part of this attack, the adversary circumvents the content editing restrictions of an OSN by using redirect links.



Figure 1: Chameleon Attack Phases.

We align the phases of a typical *Chameleon* attack to a standard cyber kill chain as follows:

1. **Reconnaissance** (out of scope): The attacker collects information about the victim using standard techniques to create an appealing disguise for the *Chameleon* posts and profiles.
2. **Weaponizing** (main phase): The attacker creates one or more redirection chains to Web resources (see Required Resources in Section 3.2). The attacker creates *Chameleon* posts or profiles that contain the redirect links.
3. **Delivery** (out of scope): The attacker attracts the victim’s attention to the *Chameleon* posts and profiles, similar to phishing or spear-phishing attacks.
4. **Maturation** (main phase): The *Chameleon* content builds trust within the OSN, collects social capital, and interacts with the victims. This phase is inherent to spam and phishing attacks that employ fake OSN profiles. But since such attacks are not considered as sophisticated and targeted, this phase is typically ignored in standard cyber kill chains or is referred to by the general term of *social engineering*. Nevertheless, building trust within an OSN is very important for the success of both targeted and un-targeted *Chameleon* attacks.
5. **Execution** (main phase): The attacker modifies the display of the *Chameleon* posts or profiles by changing the redirect target and refreshing the cached link previews.

Since the *Chameleon* attack is executed outside the victim’s premises there are no lateral movement or privilege escalation cycles. This attack can be used during the reconnaissance phase of a larger attack campaign or to reduce the cost of weaponizing any OSN based attack campaign (see examples in Section 3.3). The most important phases in the execution flow of the *Chameleon* attack are *weaponizing*, *maturation*, and *execution* as depicted in Figure 1. The attacker may proceed with additional follow-up activities depending on the actual attack goal as described in Section 3.3.

⁰The authors would like to thank the icons website (<https://icons8.com>)

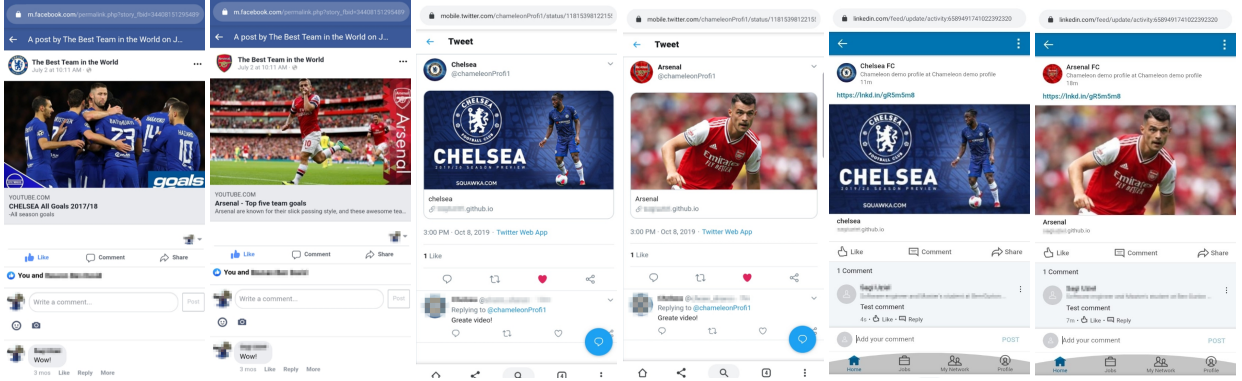


Figure 2: Changing post display in Facebook, Twitter, and LinkedIn (from left to right)

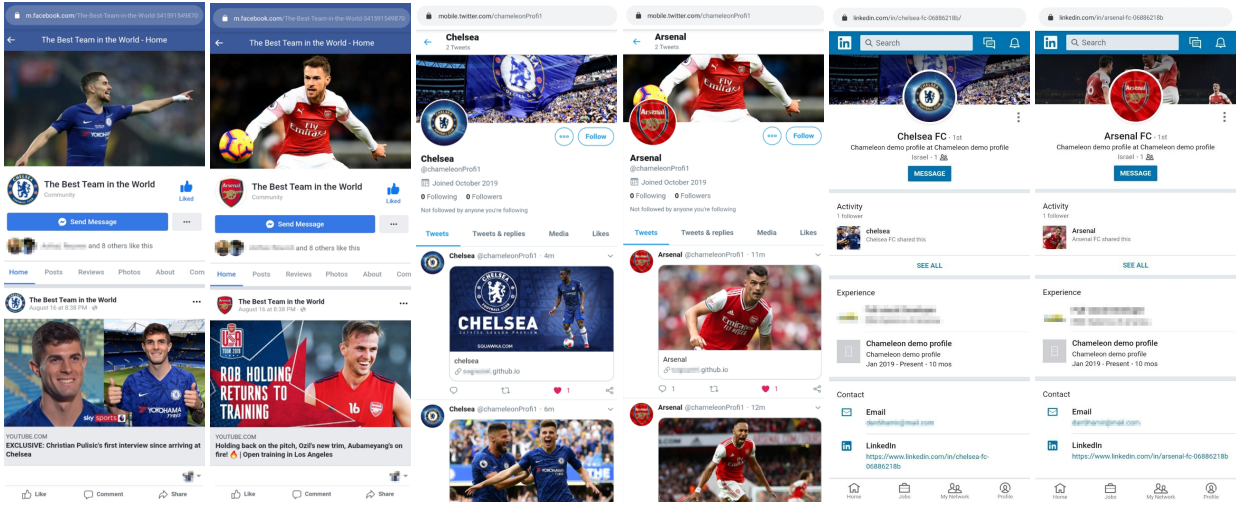


Figure 3: Changing page display in Facebook, Twitter, and LinkedIn (from left to right)

3.1 A Brief Showcase

In order to demonstrate how a *Chameleon* attack looks from the user's perspective, we show here examples of *Chameleon* posts and *Chameleon* profiles.¹

The link preview in this post will change each time you click the video. It may take about 20 seconds and requires refreshing the page.

Chameleon Post Figures 2 (1,2) present the same post on Facebook with two different link previews. Both versions of the post lead to YouTube.com and are displayed accordingly. There is no indication of any modification made to the post in either of its versions because the actual post was not modified. Neither is there an edit history, for the same reason. Likes and comments are retained. If the post was shared, the shares will show the old link preview even after it was modified in the original post.

Similarly, Figure 2 (3,4) and (5,6) present two versions of the same post on Twitter and LinkedIn respectively. There is no edit indication nor edit history because Twitter tweets cannot be edited. As with Facebook, likes, comments, and retweets are retained after changing the posted video and updating the link preview. Unlike Facebook, however the link previews of all retweets and all LinkedIn posts that contain the link will change simultaneously.

Chameleon Profile Figure 3 presents example of a *Chameleon* page on Facebook and a *Chameleon* profile on Twitter. Since the technique used to build *Chameleon* profiles and *Chameleon* pages are similar as well as their look and feel, in

¹A demo *Chameleon* post is available at https://www.facebook.com/permalink.php?story_fbid=101149887975595&id=101089594648291&__tn__=-R

the rest of this paper we will use the terms pages and profiles interchangeably. All OSNs allow changing the background picture and the description of profiles, groups, and pages. A *Chameleon* profile is different from a regular profile by *Chameleon* posts included alongside neutral or personal posts. This way a Chelsea fan (Figure 3.1) can pretend to be an Arsenal fan (Figure 3.2) and vice versa.

3.2 Required Resources

The most important infrastructure element used to execute the *Chameleon* attack is a redirection service that allows the attacker to modify the redirect target without changing the alias. This can be implemented using a link redirection service or a website controlled by the adversary. For the attack to succeed in the former case, the link redirection service must allow modifying the target link for a previously defined alias. This is the preferred infrastructure to launch the *Chameleon* attack.

In the latter case, if the attacker has control over the redirection server then a server-side 301 redirect can be used, seamlessly utilizing the link preview feature of major OSNs. If the attacker has no control over the web server, he/she may still use a client-side redirect. He/she will have to supply the required metadata for the OSN to create link previews.

If the attacker owns the domain name used to post the links, he/she may re-target the IP address associated with the domain name to a different web resource. Fast flux attack infrastructure can also be used; however, this is overkill for the *Chameleon* attack and may cause the attack to be detected [10].

3.3 Example Instances

In this section, we detail several examples of misuse cases [11] which extend the general *Chameleon* attack. Each misuse case provides a specific flavor of the attack execution flow, as well as the possible impact of the attack.

3.3.1 Incrimination and Shaming

This flavor of the *Chameleon* attack targets specific users. Shaming is one of the major threats in OSNs [12]. Its impact can be greatly amplified if the adversary employs chameleons and the victim is careless enough to interact with content posted by a dubious profile or page.

Execution flow The attacker performs the (1) *reconnaissance* and (3) *delivery* phases using standard techniques, similar to a spear-phishing attack.²

(2) During the *weaponizing* phase, the attacker creates *Chameleon* posts that endorse a topic favored by the victim. For example, he/she may post some new clips of music by the victim’s favorite band. Each post includes a redirect link that points to an appropriate YouTube video or similar Web resource, but the redirection is controlled by the attacker.

(4) During the *maturation* phase, the victim shows their appreciation of seemingly appealing content by following the *Chameleon* page, linking, retweeting, commenting, or otherwise interacting with the *Chameleon* posts. Unlike in spear-phishing where the victim is directed to an external resource or is required to expose his/her personal information, here standard interactions that are considered safe within OSNs are sufficient to affiliate the victim with the *Chameleon* posts. This significantly lowers the attack barrier.

(5) Finally, immediately after the victim’s interaction with the *Chameleon* posts, the adversary switches their display to content that opposes the victim’s agenda in order to cause maximal embarrassment or political damage. The new link preview will appear in the victim’s timeline. The OSN will amplify this attack by notifying the victim’s friends (Facebook) and followers (Twitter) about the offensive posts liked, commented, or retweeted by the victim.

Potential impact At the very least, such an attack can cause discomfort to the victim. It can be life-threatening in cases when the victim is a teenager. And it can have far-reaching consequences if used during political campaigns.

3.3.2 Long Term Avatar Fleet Management

Adversaries maintain fleets of fake OSN profiles termed avatars in order to collect intelligence, infiltrate organizations, disseminate misinformation, etc. In order to avoid detection by machine learning algorithms and build long term trust within the OSN sophisticated avatars need to be operated by a human [13, 14]. The maturation process of such avatars

²Here and in the rest of this section, numbers in parentheses indicate the attack phases in the order they are performed in each misuse case.

may last from several months to a few years. Fortunately, the attack target and the required number of avatars are usually not known in advance significantly reducing the cost-effectiveness of sophisticated avatars.

Chameleon profiles exposed in this article facilitate efficient management of a fleet of avatars by maintaining a pool of mature avatars whose timeline can be adapted to the agenda of the attack target once it is known.

Execution Flow In this special misuse case the attack phases *weaponizing* and *maturation* are performed twice; both before and after the attack target is known.

(1) The first *weaponizing* phase starts with establishing the redirect infrastructure and building a fleet of avatars. They are created with neutral displays common within the OSN.

(2) During the initial *maturation* process the neutral avatars regularly publish *Chameleon* posts with neutral displays. They acquire friends within the OSN while maximizing the acceptance rate of their friend requests [14].

(3) Once the attack target is known the attacker performs the required *reconnaissance*, selects some of the mature *Chameleon* profiles, and (4) *weaponizes* them with the relevant agenda by changing the profile information and the display of all past *Chameleon* posts.

During (5) *delivery* and (6) the second *maturation* phase the refreshed *Chameleon* profiles (avatars) contact the target and build trust with it. The (7) *execution* phase in this misuse case depends on the attacker’s goals. It is likely that the avatars that already engaged in an attack will be discarded.

Potential Impact It’s unnecessary for the adversary to create an OSN account and build an appropriate agenda for each avatar long before executing an attack. *Chameleon* profiles and posts are created and maintained as a general resource suitable for various attack campaigns. As a result, the cost of maintaining such avatars is dramatically reduced. Moreover, if an avatar is detected and blocked during the attack campaign, its replacement can be *weaponized* and released very quickly.

3.3.3 Evading Censorship

OSNs maintain millions of entities, such as pages, groups, communities, etc. For example, Facebook groups unite users based on shared interests [15]. In order to ensure proper language, avoid trolling and abuse, or allow in only users with a very specific agenda, moderators inspect the users who ask to join the groups and review the published posts. *Chameleon* attack can help in evading censorship, as well as a shallow screening of OSN profiles. See Section 4.3 for specific recommendations on profile screening to detect *Chameleon* profiles.

For example, assume two Facebook groups, uniting Democrat and Republican activists during USA elections. Assume a dishonest activist from one political extreme that would like to join a Facebook group of the rivals. Reasons may vary from trolling to spying. Assume, that this activist would like to spread propaganda within the rival group. But pages that exhibit an agenda that is not appropriate for the group would not be allowed by the group owner. The next procedure would allow the rival activist to bypass the censorship of the group moderator.

Execution Flow During the (1) *reconnaissance* phase, the adversary learns the censorship rules of the target. (2) The *weaponizing* phase includes establishing a *Chameleon* profile with agenda appropriate to the censorship. During the (3) *maturation* phase, the adversary publishes posts with redirect links to videos fitting the censorship rules. (4) *delivery* in this case represents the censored act such as requesting to enter a group, sending a friend request, posting a video, etc. The censor, e.g. the group’s administrator, reviews the profile and its timeline and approves them to be presented to all group members. Finally, in the (5) *execution* phase, the adversary changes the display of its profile and posts to reflect a new agenda that would otherwise not be allowed by the censor.

Potential Impact This attack allows the adversary to infiltrate a closed group and publishing posts in contrast to the administrator’s policy. Moreover, one-time censorship of published content would no longer be sufficient. Moderators would have to invest a lot more effort in the periodical monitoring of group members and their posts to ensure that they still fit the group’s agenda. In Section 5, we demonstrate the execution of the *Chameleon* attack for penetrating closed groups using soccer fan groups as an allegory for groups with extreme political agenda.

3.3.4 Promotion

Unfortunately, the promotion of content, products, ideas, etc. using bogus and unfair methods is very common in OSNs. Spam and crowdturfing are two example techniques used for promotion. The objective of spam is to reach maximal exposure through unsolicited messages. Bots and crowdturfers are used to misrepresent the promoted content

as a generally popular one by adding likes and comments. Crowdturfers [16] are human workers who promote social content for economic incentives. *Chameleon* attack can be used to acquire likes and comments of genuine OSN users by piggybacking a popular content.

Execution Flow During (1) *reconnaissance* phase, the attacker collects information about a topic favorable to the general public that is related to the unpopular content that the attacker wants to promote. (2) During the *weaponizing* phase, the attacker creates *Chameleon* page and posts that support the favorite topic. For example, assume an adversary who is a new singer who would like to promote themselves. In the *weaponizing* phase, he/she can create a *Chameleon* page that supports a well-known singer. During the (3) *delivery* and (4) *maturation* phases, the OSN users show their affection towards seemingly appealing content by interacting with the *Chameleon* page using likes, linking, retweeting, commenting, etc. As time passes, the *Chameleon* page obtains social capital. In the final (5) *execution* phase, the *Chameleon* page’s display changes to support the artificially promoted content retaining the unfairly collected social capital.

Potential Impact The attacker can use *Chameleon* pages and posts to promote content in OSNs by piggybacking popular content. The attacker enjoys the social capital provided by a genuine crowd that otherwise would not interact with the dubious content. Social capital obtained from bots or crowdturfers can be down-rated using various reputation management techniques. In contrast, social capital obtained through the *Chameleon* trickery is provided by genuine OSN users.

3.3.5 Clickbait

Most of the revenues of online media come from online advertisements [17]. This phenomenon generated a significant amount of competition among online media websites for the readers’ attention and their clicks. To attract users and encourage them to visit a website and click a given link, the website administrators use catchy headlines along with the provided links, which lure users into clicking on the given link [17]. This phenomenon titled clickbait.

Execution Flow (1) During the *weaponizing* phase, the attacker creates *Chameleon* profiles with posts with redirect links. Consider an adversary that is a news provider who would like to increase the traffic to its website. To increase its revenues, he can do the following: in the *weaponizing* phase, he should publish a *Chameleon* post with a catchy headline with an attached link to an interesting article. Later, in the *maturation* phase, users attract the post by its attractive link preview, as well as its headline, and increase the traffic to a website. Later, in the *execution* phase, the adversary changes the redirect target of the posted link but keeping the link preview not updated. As a result, new users will click on the *Chameleon* post that its display did not change, but now they will be navigated to the adversary’s website.

Potential Impact By applying this attack, the attacker can increase his traffic and, eventually, his income. Luring the users with an attractive link preview in which increases the likelihood that the user will click on it and will consume his content.

4 Susceptibility of Social Networks to the Chameleon Attack

4.1 Online Social Networks

We review the susceptibility of seven OSNs to the *Chameleon* attack.

4.1.1 Facebook

Alongside its growing popularity, Facebook allows users to manipulate the display of previously published posts based on several different features. The features include the publishing of redirect links, editing post’s publication date, hiding previously published posts, and publishing unauthorized content in a closed group.

Up until 2017, in case a user edits a post on Facebook, an indicator is presented for the users to notify them that the content had been updated. After 2017, a Facebook update removed this public notification and enable to see the post’s history only via the button of ‘View Edit History’.

While Facebook allows editing post’s publication date, it displays a small indication concerning the original publication date of the post. To watch the original publication date, a user must hover over the clock icon shown in the post, and a bubble will be shown together with the original publication date.

Table 1: Features that facilitate and mitigate the *Chameleon* attack in popular OSNs.

Attacker’s ability	OSN feature	Facebook	Twitter	WhatsApp	Instagram	Reddit	Flickr	LinkedIn
Creating artificial timeline	Editing a post’s publication date	Y 🚫	N 🟢	N 🟢	N 🟢	N 🟢	N 🟢	N 🟢
	Presenting original publication date	Y 🟢	-	-	-	-	-	-
Changing content	Editing previously published posts	Y 🚫	N 🟢	N 🟢	Y 🚫	Y 🚫	Y 🚫	Y 🚫
	Indication in edited published posts	Y 🟢	-	-	Y 🟢	N 🚫	N 🚫	Y 🟢
	Indication in edited shared posts	N 🚫	-	-	Y 🟢	-	-	Y 🟢
	Presenting edit history	Y 🟢	-	-	N 🚫	-	-	N 🚫
Changing display	Publishing redirect links	Y 🚫	Y 🚫	Y 🚫	N 🟢	Y 🚫	Y 🚫	Y 🚫
	Displaying link preview	Y 🚫	Y 🚫	Y 🚫	-	Y 🚫	N 🟢	Y 🚫
	Updating link preview	Y 🚫	Y 🚫	N 🟢	-	N 🟢	-	Y 🚫
Switching content	Hiding posts	Y 🚫	N 🟢	N 🟢	Y 🚫	Y 🚫	Y 🚫	N 🟢

🚫= Facilitates the *Chameleon* attack. 🟢= Mitigates the *Chameleon* attack

Also, concerning Facebook pages, Facebook does not allow to do radical changes to the original name of a page daily. However, it is still possible to conduct limited edits to the page’s name; changes that are so minor that the context of the original name will be not changed. As a result, we were able to rename a page in phases by editing the name of a given page with small changes in each edit action. First, we changed only two characters from the name of a page. Afterward, three days later, we changed two more characters and so forth until eventually, we were able to rename the page entirely as we wished.

Facebook employs a mechanism called Link Shim to keep Facebook users safe from external malicious links [18]. When clicking on an external link posted on Facebook, their mechanism checks if the link is blacklisted. In case of a suspicious URL, Facebook will display a message to the user [18]. Redirect links used in *Chameleon* posts lead to legitimate destinations and so are currently approved by Link Shim.

4.1.2 Twitter

As opposed to Facebook, Twitter does not allow users to edit and hide tweets that have already been published, or to manipulate a tweet’s publication date (see Table 1). This mechanism makes it more difficult for an attacker to manipulate the display of previously published content. On the other hand, Twitter allows the use of client redirects. This poses the same danger as Facebook redirects, allowing attackers to manipulate the link preview of a tweet with content that is not necessarily related to the target website. Moreover, Twitter allows users to update a link preview using the *Card Validator*.³ In addition, Twitter makes it possible to change a user’s display name but does not allow to change the original username chosen during registration (serves as an identifier).

4.1.3 WhatsApp

WhatsApp allows messages to be published with redirect links and it displays link previews but it does not allow the update of an already published link preview. As opposed to other OSNs, WhatsApp is the only OSN that displays an indication that the message was deleted by its author.

WhatsApp is safe against most flavors of the *Chameleon* attack, except *clickbait* where an attacker can trick other users by encouraging them to click a malicious link with a preview of a benign link.

4.1.4 Instagram

Concerning redirect links, Instagram does not allow users to publish external links (see Table 1). Since the posts on Instagram are based on images, it is not an option for the attacker to change the published content by redirect link. However, Instagram allows to edit already published posts. The editing process includes the text in the description section, as well as the image itself. In case of such a change to a post was made by its owner, no indication is shown to users.

4.1.5 Reddit

Alongside its popularity, Reddit is prone to a *Chameleon* attack: In this OSN, the attacker can edit, delete or hide already published posts while others will not be able to know that the content has been modified.

³ <https://cards-dev.twitter.com/validator>

4.1.6 Flickr

As opposed to Facebook and WhatsApp, Flickr does not show link previews, but it allows users to update their posts, replace uploaded images, hide already published posts, and edit their account name. All these activities can be performed by users, without any indication for the users to the editing activity.

4.1.7 LinkedIn

LinkedIn permits users to share a redirect link, and to update the link preview using *Post Inspector*.⁴ As a result, users can edit their posts, however, the post will be marked as edited.

4.2 Existing Weaknesses and Security Controls

Next, we summarize the OSN weaknesses related to the *Chameleon* attack, as well as controls deployed by the various OSNs to mitigate potential misuse. While the main focus of this article is the *Chameleon* attack facilitated by cached link previews, in this subsection we also discuss other types of the *Chameleon* attack successfully mitigated by major OSNs.

4.2.1 Creating artificial timeline

Publishing posts in retrospective is a feature that is easiest to misuse. Such a feature helps an adversary creating OSN accounts that look older and more reliable than they are. Luckily, all OSNs, but Facebook, do not provide such a feature to their users. Although Facebook allows *editing a post's publication date*, it mitigates possible misuse of this feature for creating artificial timelines by *presenting the original publication date* of the post.

4.2.2 Changing content

Some OSNs provide their users with the ability to *edit previously published posts*. This feature facilitates all misuse cases detailed in Section 3.3 without any additional resources required from the attacker. Twitter and WhatsApp do not allow editing of previously published posts. Facebook, Instagram, and LinkedIn mitigate potential misuse by *presenting editing indication in published posts*. Facebook even *presents the edit history* of a post. Unfortunately, in contrast to Instagram and LinkedIn, Facebook does not *present the edit indication in shared posts*. We urge Facebook to correct this minor yet important omission.

4.2.3 Changing Display

The primary weakness of the major OSNs (Twitter, Facebook, and LinkedIn) which facilitates the *Chameleon* attack discussed in this paper is the combination of three features provided by the OSNs. First, *publishing redirect links* allows attackers to change the navigation target of the posted links without any indication of such a change. Second, OSNs *display a link preview* based on metadata provided by the website at the end of the chain of server redirects. This feature allows the attackers to control the way link previews are displayed. Finally, OSNs allow *updating link preview* following the changes in the redirect chain of the previously posted link. Such an update is performed without displaying an indication that the post was updated. Currently, there are no controls that mitigate the misuse of these features.

WhatsApp, Reddit, and LinkedIn display link previews of redirect links similar to Facebook and Twitter. But they do not provide a feature to update the link previews. On one hand, the only applicable misuse case for the *Chameleon* attack in these OSNs is *clickbait*. On the other hand, updating link previews is important for commercial brand management.

4.2.4 Switching Content

Facebook, Instagram, Reddit, and Flickr allow users to temporarily *hide their posts*. This feature allows a user to prepare multiple sets of posts where each set exhibits a different agenda. Later, the adversary may display the appropriate set of posts and hide the rest. The major downsides of this technique as far as the attacker is concerned are: (1) The need to maintain the sets of posts ahead of time similar to maintaining a set of regular profiles. (2) Social capital acquired by one set of posts cannot be reused by the other sets, except friends and followers.

Overall all reviewed OSNs are well protected against timeline manipulation. The major OSNs, except Reddit and Flickr, are aware of the dangers of post-editing and provide appropriate controls to avoid misuse. Due to the real-time nature of messaging in Twitter and WhatsApp, these OSNs can disable the option of editing posts.

⁴ <https://www.linkedin.com/post-inspector>

The major OSNs, Facebook, Twitter, and LinkedIn, really care about the business of their clients and thus, explicitly provide features to update link previews. *Chameleon* attack exposed in this paper misuses this feature to manipulate the display of posts and profiles. Provided that Reddit and Flickr allow editing the post content, only WhatsApp and Instagram are not susceptible to *Chameleon* attacks.

Instagram stores the posted images and not the links to the external resources, an approach that may not scale and may not be suitable for all premium customers. WhatsApp stores the data locally and does not allow recollecting past messages if the receiver is not a member of the group when the message was posted. Clearly, WhatsApp’s approach is not suitable for bloggers, commercial pages, etc. that would like to share their portfolio with every newcomer.

4.3 Additional Required Security Controls

The best way to mitigate the *Chameleon* attack is to disallow redirect links and to disable link preview updates in all OSNs. Nevertheless, we acknowledge that it is not possible to stop using external redirect links and short URLs. These features are very popular on social networks and important in brand management.

First and foremost an appropriate change indication should be displayed whenever the link preview cache is updated. Since on Facebook the cache is updated by the author of the original post, this act can naturally be displayed in the edit history of the post. Link preview cache updates should be treated similar to the editing of posts.

However, edit indications on posts won’t help unless OSN users will be trained to pay attention to these indications. Facebook, and other OSNs, should make it crystal clear which version of the post a user liked or commented on. To minimize the impact of the *Chameleon* attack likes, shares and comments of a post should be associated with a specific version of the post within the edit history, by default. It is also important to let users know about subsequent modifications of the posts they liked, commented, or shared. The users will be able, for example, to delete their comments or to confirm it, moving the comment back from the history to the main view.

In Twitter and LinkedIn, anyone can update the link preview. The motivation for this feature is two-fold: (1) The business owner should be able to control the look and feel of his business card within the OSN regardless of the specific user who posted it. (2) Link previews should always be up to date. It will be challenging to design appropriate mitigation for the *Chameleon* without partially giving up these objectives.

We suggest notifying a Twitter (or LinkedIn) user who posted a link to an external site whenever the link preview is updated. The user will be able to delete the post or accept the link preview update at his sole discretion. By default, the link preview should remain unchanged. This approach may increase the number of notifications the users receive, but with appropriate filters, it will not be a burden on the users. However, it may require maintaining copies of link previews for all re-posted links, which in turn significantly increase storage requirements.

Finally, OSNs should update their anomaly detection algorithms to take into account changes made to the posts’ content and link previews as well as the reputation of the servers along the redirection path of the posted links.

It may take time for the OSNs to implement the measures described above. Meanwhile, users should be aware that their *likes and comments are precious assets* that may be used against them if given out blindly.

Next, we suggest a few guidelines that will help average OSN users detecting *Chameleon* posts and profiles. Given a suspected profile, check the textual content of its posts. *Chameleon* profiles should publish general textual descriptions to easily switch agenda. The absence of opinionated textual descriptions in the topic of your mutual interest may indicate potential *Chameleon*. A Large number of ambiguous posts that can be interpreted in the context of the cover image or in the context of other posts in the timeline should increase the suspicion. For example, “This is the best goalkeeper in the world!!!” without a name mentioned is ambiguous. Also using public services like Facebook provided⁵ for watching a given post history can be useful for detecting a *Chameleon* post.

A large number of redirect links within the profile timeline is also an indication of *Chameleon* capabilities. We do not encourage the users to click links in the posts of suspicious profiles to check whether they are redirected! In Facebook and LinkedIn, a simple inspection of the URL can reveal whether a redirection is involved. Right-click the post and copy-paste the link address in any URL decoder. If the domain name within the copied URL matches the domain name within the link preview and you trust this domain, you are safe. Today, most links on Facebook are redirected through Facebook’s referral service. The URL you should look at follows the “u” parameter within the query string of l.facebook.com/l.php. If the domain name is appearing after “, u=” differs from the domain name within the link preview, the post author uses redirection services. Unfortunately, today, links posted on Twitter are shortened, and the second hop of the redirection cannot be inspected by just copying the URL.

⁵ <https://developers.facebook.com/tools/debug/sharing/batch/>

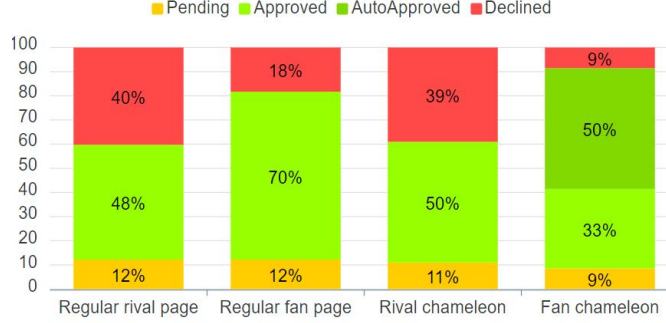


Figure 4: Request results by type of page

5 Group Infiltration Experiment

In this section, we present an experiment conducted on Facebook to assess the reaction of Facebook group moderators to *Chameleon* pages. In this experiment, we follow the execution flow of the misuse case number 4 *evading censorship* in Section 3.3.

5.1 Experimental Setup

In this experiment, four pairs of rival soccer and basketball teams were selected: Arsenal vs Chelsea, Manchester United vs Manchester City, Lakers vs Clippers, and Knicks vs Nets. We used sixteen Facebook pages: one regular and one *Chameleon* page for each sports team. Regular pages post YouTube videos that support the respective sports team. Their names are explicitly related to the team they support e.g. “Arsenal - The Best Team in the World”. *Chameleon* pages post redirect links that lead to YouTube videos that support either the team or their rivals. Their names can be interpreted based on context e.g. “The Best Team in the World”. The icons and cover images of all pages reflect the team they (currently) support.

Next, we selected twelve Facebook groups that support each one of the eight teams (total of 96 Facebook groups) according to the following three criteria: (a) the group allows pages to join it, (b) the group is sufficiently large (at least 50 members), and (c) there was at least some activity within the group in last month.

We requested to join each group four times: (1) as a regular fan page, (2) as a regular rival page, (3) as a *Chameleon* page while supporting the rivals, and (4) the same *Chameleon* page requested to join the group again now pretending to be a fan page. We requested each group in a random order of the pages. We used balanced experiment design to test all permutations of pages where the respective *Chameleon* page first requests to join the group as rival’s page and afterward as fan’s page. We allowed at least five days between consequent requests to join each group.

A page can be *Approved* by the group admin or moderator (hereafter admin). In this case the page becomes a member of the group. While the admin have not decided yet, the request is *Pending*. The owner can *Decline* the request. In this case the page is not a member of the group, but it is possible to request to join the group again. Neither one of our pages was *Blocked* by the group admins, therefore, we ignore this status in the following results. Whenever, *Chameleon* page pretending to be a rival page is *Approved* by an admin, there is no point in trying to join the same group using the same page again. We consider this status as *Auto Approved*.

The first phase of the experiment started on July 20, 2019 and included only the Facebook groups supporting Chelsea and Arsenal. The relevant *Chameleon* pages changed the way they are displayed on Aug. 16. The second phase started on Sept. 5, 2019 and included the rest of the Facebook groups. The relevant *Chameleon* pages changed the way they are displayed on Sept. 23. The following results summarize both phases.

5.2 Results

During the experiment, 14 Facebook groups decided to prevent (any) pages from joining the group. We speculate that the admins were not aware to the option of accepting pages as group members, and updated the group settings after they saw our first requests. These 14 groups were *Disqualified* in current experiment. Overall there were 206 *Approved* requests, 87 *Declined*, and 35 *Pending*. Figure 4 presents the distribution of request statuses for the different types of pages.

Some admins blindly approve requests. For example, 28 groups approved all requests. Other group admins meticulously check the membership requests. Thirteen groups *Declined* or ignored the rival pages and *Approved* pages that exhibit the correct agenda.

Overall **the reaction of admins to *Chameleon* pages is similar to their reaction to regular pages with the same agenda.** To check this hypothesis we used a one-way ANOVA test to determine whether there is a significant difference between the four types of group membership requests. The test was conducted on the request status values at the end of the experiment (*Declined*, *Pending*, *Approved*). Results showed that there is no statistically-significant difference between the approval of *Chameleon* fan pages and regular fan pages (p-value = 0.33). There is also no statistically-significant difference between the approval of *Chameleon* rival pages and regular rival pages (p-value = 0.992). However, the difference between approval of either regular or *Chameleon* rival pages and the approval of both types of fan pages is statistically-significant with p-value ranging from 0.00 to 0.003. These results indicate that the reaction of admins to *Chameleon* pages in our experiment is similar to their reaction to regular (non-chameleon) pages with a similar agenda. We conclude that **admins do not distinguish between regular and *Chameleon* pages.** This conclusion is stressed by the observation that only two groups out of 82 *Declined Chameleon* fan pages and *Approved* regular fan pages. Seven groups approved *Chameleon* fan pages and rejected regular fan page.

The above results also indicate that, in general, **admins are selective toward pages that they censor.** Next, we measure the selectivity of the group admins using Likert scale [19]. Relying on the conclusion that admins do not distinguish between regular and *Chameleon* pages, we treat them alike to measure admins' selectivity. Each time a group admin *Declined* a rival page or *Approved* a fan page he/she received one point. Each time a fan page was *Declined* or a rival page was *Approved*, the selectivity was reduced by one point. *Pending* request status added zero toward the selectivity score.

For each group, we summed up the points to calculate its selectivity score. When selectivity score is greater than three, we consider the group as *selective*. If the selectivity score is less than or equal to three, we consider the group as *not selective*.

To explain the differences in groups' selectivity we first tested whether there is a difference between the number of members in selective and non-selective groups using t-tests. We found that smaller groups are more selective than, larger ones with (p-value = 0.00029). This result is quite intuitive. Smaller groups tend to check the identity of the users who ask to join the group, while large groups are less likely to examine the identity of the users who want to join the group. Figure 5 presents the groups' activity and size vs. their selectivity score. There is a weak negative correlation between group's selectivity score and number of members (Pearson correlation = -0.187, p-value = 0.093).

6 Related Work

6.1 Content Spoofing and Spoofing Identification

Content spoofing, also known as content injection or virtual defacement, is an attack method that deceives users in assuming that particular content on a web site is legitimate and not from an external source [20, 21, 22]. Using this attack, an attacker can upload new, fake, or modified content to the web site as legitimate. Content Spoofing can lead to malware exposure, financial fraud, or privacy violations, and can misrepresent an organization or an individual [23, 24]. Content spoofing usually exploits the trust relationship between a web application and its users as the modified web page is presented to the user under the context of the application domain [25].

According to WhiteHat [26], content spoofing is one of the most prevalent vulnerabilities in web applications. The content spoofing attack leverages the code injection vulnerability where the user's input is not sanitized correctly. Using this vulnerability, an attacker can provide new content to the web, usually via the GET or POST parameter. Hussain et al. [25] present two ways to conduct content spoofing attack. An HTML Injection, in which the attacker alters the content of a web page for malicious purposes by using HTML tags, or a Text Injection that manipulates the text data of a parameter.

Jitpukdebodin et al. [27] introduce a new technique that explores vulnerability in WLAN communication. The proposed method creates a crafting spoof web content and sends it to a user before the genuine web content from a website is transmitted to the user. Hussain et al. [25] present a new form of compounded SQL injection attack technique which uses the SQLi attack vectors to perform content spoofing attacks on a web application.

There have been a few techniques for the detection of content spoofing attacks [24, 28]. Benea et al. [24] suggest a system to prevent content spoofing by detecting phishing attacks using fingerprints similarity. Niemela and Kesti [28] present a method for detecting unauthorized changes to a website using authorized content policy sets for each of a multiplicity of websites from the web operators and identify websites that do not conform to respective policy sets.

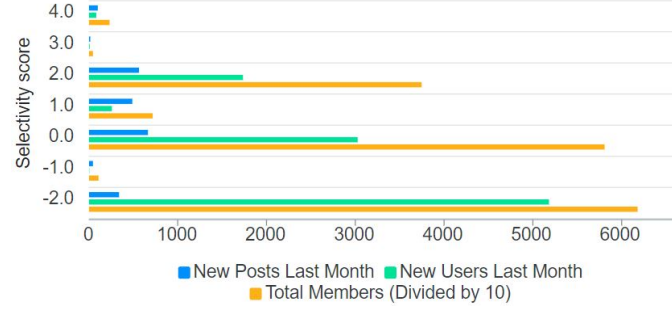


Figure 5: Average groups activity by selectivity score

6.2 Website Defacement

Website Defacement is an attack that changes the visual appearance of a website [29, 30, 31]. Using this attack, an attacker can cause serious consequences to website owners, including interrupting website operations and damaging the owner’s reputation. More interestingly, attackers may support their reputation, promoting a certain ideological, religious, or political orientation [31, 32]. Besides, web defacement is a significant threat to businesses since it can detrimentally affect the credibility and reputation of the organization [30, 33]. Most website defacement occurs when attackers manage to find any vulnerability in the Web application and then inject a remote scripting file [29].

Several types of research deal with the monitoring and detection of website defacement, with solutions that include signature-based detection [34, 35] and anomaly-based detection [30, 36, 37].

The simplest method to detect website defacement is a checksum comparison. With this method, the content of a website is calculated using hashing algorithms. The website is then monitored and a new checksum is calculated and compared with the previous one, raising an alert when the checksum is changed [29, 34, 35]. This method is effective for static web pages but not applicable to dynamic pages.

Several techniques have been proposed for website defacement based on complex algorithms [33, 38]. Kim et al. [38] propose using a 2-gram method for building a profile from normal web pages for monitoring and detecting of page defacement. Medvet et al. [33] present an approach to automatic detection of website defacement based on genetic programming. The method does not rely on any domain-specific knowledge but instead builds an algorithm based on a sequence of readings of the remote page to be monitored, and on a sample set of attacks. The remote page is then monitored at regular intervals; the algorithm is applied, which raises an alert when a suspect modification is found.

Several techniques use machine learning-based methods for website defacement detection [30, 36, 37, 39]. Those studies, build a profile of the monitored page automatically, based on machine learning techniques, and raise an alert when the page content does not fit the profile. Borgolte et al. [30] proposes the ‘MEERKAT’ detection system that requires no prior knowledge about the website content or its structure, but only its URL. ‘MEERKAT’ automatically learns high-level features from screenshots (image data) of defaced websites by machine learning, such as stacked autoencoders and deep neural networks. Results on the largest website defacement dataset achieve a high detection accuracy of over 97% and a low false-positive rate of less than 1.5%. The method’s drawback is that it requires extensive computational resources for image processing and recognition. Recently advanced research [40] proposes an application of adversarial learning to defacement detection for making the learning process unpredictable so that the adversary will be unable to replicate it and predict the classifier’s behavior using a secret key.

6.3 Cloaking attack and identification

Cloaking, also known as ‘bait and switch’ is a common technique used to hide the true nature of a Web site by delivering different semantic content to some selected specific user group-based [41, 42]. Wang and Savage [41] presented four cloaking types: Repeat cloaking (delivering different web content based on visit times of visitors), User-agent cloaking (delivering specific web content based on visitors’ User-agent String), Redirection cloaking (redirecting users to another website by using JavaScript), and IP Cloaking (delivering specific web content based on visitors’ IP).

Researchers have responded to the cloaking techniques with a variety of anti-cloaking techniques [42]. Basic techniques relied on a cross-view comparison technique [43, 44]. A page is classified as cloaking if the redirect chain deviated across fetches. Other approaches mainly target compromised web servers and identify clusters of URLs with trending keywords that are irrelevant to the other content hosted on page [45]. Wang et al. [41] identify cloaking in near real-time

by examining the dynamics of cloaking over time. Invernizzi et al. [42] develop an anti-cloaking system that detects split-view content returned to two or more distinct browsing profiles by building a classifier that detects deviations in the content.

6.4 Manipulating Human Behavior

These days, cyber-attacks manipulate human weaknesses more than ever [46]. Our susceptibility to deception, an essential human vulnerability, is a significant cause of security breaches. Attackers can exploit the human vulnerability by sending a specially crafted malicious email, tricking humans into clicking on malicious links, and thus downloading malware, (a.k.a. spear phishing) [47].

One of the main attack tools that exploit the human factor is social engineering, which is defined as the manipulation of the human aspect of technology using deception [48]. Social engineering plays on emotions such as fear, curiosity, excitement, and empathy, and exploits cognitive biases [49]. The basic 'good' human nature characteristics make people vulnerable to the techniques used by social engineers, as it activates various psychological vulnerabilities, which could be used to manipulate the individual to disclose the requested information [50, 51, 52, 53]

The exploitation of the human factor has extensive use in advanced persistent threats (APTs). An APT attack involves sophisticated and well-resourced adversaries targeting specific information in high-profile companies and governments [54]. In APT attacks, social engineering techniques are aimed at manipulating humans into delivering confidential information about a targeted organization or getting an employee to take a particular action (e.g., executing malware) [14, 55, 56].

To the best of our knowledge, the *Chameleon* attack was previously executed in files during content-sniffing XSS attacks [57] but not on the social media platform. Chameleon documents discussed by Barth et al. are files conforming to multiple file formats (e.g. PostScript+HTML). The attack exploits the fact that browsers can parse documents as HTML and execute any hidden script within. In contrast to chameleon documents, which are parsed differently by different tools without adversarial trigger, our chameleon posts are controlled by the attacker and are presented differently to the same users at different times.

7 Conclusions and Future Work

This article discloses a weakness in an important feature provided by three major OSNs: Facebook, Twitter, and LinkedIn, namely *updating link previews without visible notifications while retaining social capital* (e.g., likes, comments, retweets, etc.). This weakness facilitates a new *Chameleon* attack where the link preview update can be misused to damage the good name of users, avoid censorship, and perform additional social networks scam detailed in Section 3.3. Out of seven reviewed social networks, only Instagram and WhatsApp are resilient against most flavors of the *Chameleon* attack.

We acknowledge the importance of the link preview update feature provided by the OSNs to support businesses that disseminate information through social networks and suggest several measures that should be applied by the OSNs to reduce the impact of *Chameleon* attacks. The most important measure is binding social capital to the version of a post to which it was explicitly provided. We also instruct OSN users on how to identify possible chameleons.

We experimentally show that even the most meticulous Facebook group owners fail to identify *Chameleon* pages trying to infiltrate their groups. Thus it is extremely important to raise the awareness of OSN users to this new kind of trickery.

We encourage researchers and practitioners to identify potential *Chameleon* profiles throughout the OSNs in the nearest future; develop and incorporate redirect reputation mechanisms into machine learning methods for identifying social network misuse; and include the *Chameleon* attack in security awareness programs alongside phishing scam and related scam.

8 Ethical and Legal Considerations

Our goal is hardening OSNs against misuse while respecting the needs and privacy of OSN users. We believe that it is important to raise the awareness of researchers, practitioners, OSN operators and users to the potential misuse of link previews. We follow strict Responsible Full Disclosure Policy, as well as guidelines recommended by the Ben-Gurion University Human Subject Research Committee.

In particular, we did not access or store any information about the profiles we contacted during the experiment. We only recorded the status of the requests to join their Facebook groups. The *Chameleon* pages used during the experiment are

deleted at the end of the study. Owners of the contacted Facebook groups are able to decide whether or not to accept the request from our pages. Although we did not inform them about the study prior to the requests, they are provided with post-experiment written feedback regarding their participation in the trial, as well as guidelines to safeguard themselves from *Chameleon* attacks and other OSN scam. We contact the relevant OSNs at least one month prior to publication of the trial results and disclosure of the related weaknesses. No rules or agreements were violated in the process of this study. In particular, we use Facebook pages in the showcase and in the experiment rather than profiles in order to adhere to the Facebook End-User Licence Agreement.

9 Availability

Chameleon pages, posts, and tweets are publicly available. Links can be found in the following GitHub repository: <https://github.com/aviade5/Chameleon-Attack/>.

Source code is not provided to reduce misuse. CVE and official responses of the major OSNs are also provided on the mentioned GitHub page.

References

- [1] Danah M Boyd and Nicole B Ellison. Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1):210–230, 2007.
- [2] Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon. What is twitter, a social network or a news media? In *Proceedings of the 19th international conference on World wide web*, pages 591–600. AcM, 2010.
- [3] Eric Gilbert and Karrie Karahalios. Predicting tie strength with social media. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 211–220. ACM, 2009.
- [4] Kyumin Lee, James Caverlee, and Steve Webb. Uncovering social spammers: social honeypots+ machine learning. In *Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval*, pages 435–442. ACM, 2010.
- [5] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th annual computer security applications conference*, pages 93–102. ACM, 2011.
- [6] Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici. Homing socialbots: intrusion on a specific organization’s employee using socialbots. In *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013)*, pages 1358–1365. IEEE, 2013.
- [7] Emilio Ferrara. Manipulation and abuse on social media by emilio ferrara with ching-man au yeung as coordinator. *ACM SIGWEB Newsletter*, (Spring):4, 2015.
- [8] Facebook help how to edit. <https://www.facebook.com/help/1376303972644600?helpref=related>. Accessed: 2019-09-07.
- [9] Theodorich Kopetzky and Max Mühlhäuser. Visual preview for link traversal on the world wide web. *Computer Networks*, 31(11-16):1525–1532, 1999.
- [10] Thorsten Holz, Christian Gorecki, Konrad Rieck, and Felix C Freiling. Measuring and detecting fast-flux service networks. In *NDSS*, 2008.
- [11] J McDermott. Eliciting security requirements by misuse cases. *Proc. 37th Technology of Object-Oriented Languages and Systems (TOOLS-37 Pacific 2000)*, Sydney, Australia, pages 120–131, 2000.
- [12] Lauren M Goldman. Trending now: the use of social media websites in public shaming punishments. *Am. Crim. L. Rev.*, 52:415, 2015.
- [13] Aviad Elyashar, Michael Fire, Dima Kagan, and Yuval Elovici. Guided socialbots: Infiltrating the social networks of specific organizations’ employees. *AI Communications*, 29(1):87–106, 2016.
- [14] Abigail Paradise, Asaf Shabtai, Rami Puzis, Aviad Elyashar, Yuval Elovici, Mehran Roshandel, and Christoph Peylo. Creation and management of social network honeypots for detecting targeted cyber attacks. *IEEE Transactions on Computational Social Systems*, 4(3):65–79, 2017.
- [15] Jordi Casteleyn, André Mottart, and Kris Rutten. How to use data from facebook in your market research. *International Journal of Market Research*, 51(4):439–447, 2009.
- [16] Kyumin Lee, Prithivi Tamilarasan, and James Caverlee. Crowdturfers, campaigns, and social media: Tracking and revealing crowdsourced manipulation of social media. In *Seventh International AAAI Conference on Weblogs and Social Media*, 2013.
- [17] Abhijnan Chakraborty, Bhargavi Paranjape, Sourya Kakarla, and Niloy Ganguly. Stop clickbait: Detecting and preventing clickbaits in online news media. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 9–16. IEEE, 2016.
- [18] Link shim - protecting the people who use facebook from malicious urls. <https://www.facebook.com/notes/facebook-security/link-shim-protecting-the-people-who-use-facebook-from-malicious-urls/10150492832835766/>. Accessed: 2019-12-09.
- [19] Ankur Joshi, Saket Kale, Satish Chandel, and DK Pal. Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, 7(4):396, 2015.
- [20] Ion Lungu and Alexandru Tabusca. Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. *Informatica Economica*, 14(2):27, 2010.
- [21] Nor Fatimah Awang and Azizah Abd Manaf. Detecting vulnerabilities in web applications using automated black box and manual penetration testing. In *International Conference on Security of Information and Communication Networks*, pages 230–239. Springer, 2013.

- [22] Harshal A Karandel, Pooja A Kulkarni, Shyam S Gupta, and Deepak Gupta. Security against web application attacks using ontology based intrusion detection system. *International Research Journal of Engineering and Technology (IRJET)*, 3(01):89–92, 2016.
- [23] Pedram Hayati and Vidyasagar Potdar. Spammer and hacker, two old friends. In *2009 3rd IEEE International Conference on Digital Ecosystems and Technologies*, pages 290–294. IEEE, 2009.
- [24] Robert Benea, Avneet Kaur Puri, Virgil Mihailovici, and Ravi Varanasi. Anti-content spoofing (acs), June 19 2012. US Patent 8,205,255.
- [25] Syed Zeeshan Hussain and Nancy Agarwal. Content spoofing via compounded sql injection. In *International Conference on Intelligent Computing and Communication Technologies*, pages 244–252. Springer, 2019.
- [26] Jeremiah Grossman. Whitehat website security statistics report. *Retrieved March*, 12:60, 2017.
- [27] Sumedt Jitpukdebodin, Roongroj Chokngamwong, and Supakorn Kungpisdan. A novel web content spoofing technique on wlan and its countermeasures. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)*, pages 254–258. IEEE, 2014.
- [28] Jarno Niemela and Veli-Jussi Kesti. Detecting unauthorised changes to website content, July 24 2018. US Patent App. 10/033,746.
- [29] Tushar Kanti, Vineet Richariya, and Vivek Richariya. Implementing a web browser with web defacement detection techniques. *World of Computer Science and Information Technology Journal (WCSIT)*, 1(7):307–310, 2011.
- [30] Kevin Borgolte, Christopher Kruegel, and Giovanni Vigna. Meerkat: Detecting website defacements through image-based object recognition. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 595–610, 2015.
- [31] Marco Romagna and Niek Jan van den Hout. Hacktivism and website defacement: motivations, capabilities and potential threats. In *27th Virus Bulletin International Conference*, volume 1, 2017.
- [32] Federico Maggi, Marco Balduzzi, Ryan Flores, Lion Gu, and Vincenzo Ciancaglini. Investigating web defacement campaigns at large. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 443–456. ACM, 2018.
- [33] Eric Medvet, Cyril Fillon, and Alberto Bartoli. Detection of web defacements by means of genetic programming. In *Third International Symposium on Information Assurance and Security*, pages 227–234. IEEE, 2007.
- [34] Rajiv Kumar Gurjwar, Divya Rishi Sahu, and Deepak Singh Tomar. An approach to reveal website defacement. *International Journal of Computer Science and Information Security*, 11(6):73, 2013.
- [35] Oren Shani. System and method for identification, prevention and management of web-sites defacement attacks, April 29 2010. US Patent App. 12/531,728.
- [36] Giorgio Davanzo, Eric Medvet, and Alberto Bartoli. Anomaly detection techniques for a web defacement monitoring service. *Expert Systems with Applications*, 38(10):12521–12530, 2011.
- [37] Xuan Dau Hoang. A website defacement detection method based on machine learning techniques. In *Proceedings of the Ninth International Symposium on Information and Communication Technology*, pages 443–448. ACM, 2018.
- [38] Woonyon Kim, Jeongmoon Lee, Eungki Park, and Sangwook Kim. Advanced mechanism for reducing false alarm rate in web page defacement detection. In *The 7th International Workshop on Information Security Applications*, 2006.
- [39] Alberto Bartoli and Eric Medvet. Automatic integrity checks for remote web resources. *IEEE Internet Computing*, 10(6):56–62, 2006.
- [40] Francesco Bergadano, Fabio Carretto, Fabio Cogno, and Dario Ragno. Defacement detection with passive adversaries. *Algorithms*, 12(8):150, 2019.
- [41] David Y Wang, Stefan Savage, and Geoffrey M Voelker. Cloak and dagger: dynamics of web search cloaking. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 477–490. ACM, 2011.
- [42] Luca Invernizzi, Kurt Thomas, Alexandros Kapravelos, Oxana Comanescu, Jean-Michel Picod, and Elie Bursztein. Cloak of visibility: Detecting when machines browse a different web. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 743–758. IEEE, 2016.
- [43] Yi-Min Wang and Ming Ma. Detecting stealth web pages that use click-through cloaking. In *Microsoft Research Technical Report, MSR-TR*, 2006.

- [44] Yi-Min Wang, Yi-Min Wang, Ming Ma, Yuan Niu, and Hao Chen. Spam double-funnel: Connecting web spammers with advertisers. In *Proceedings of the 16th international conference on World Wide Web*, pages 291–300. ACM, 2007.
- [45] John P John, Fang Yu, Yinglian Xie, Arvind Krishnamurthy, and Martin Abadi. deseo: Combating search-result poisoning. In *USENIX security symposium*, pages 1–15, 2011.
- [46] Bill Blunden. Manufactured consent and cyberwar. In *LockDown Conference proceedings*, 2010.
- [47] Sanjay Goel, Kevin Williams, and Ersin Dincelli. Got phished? internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2, 2017.
- [48] Sven Uebelacker and Susanne Quiel. The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust*, pages 24–30. IEEE, 2014.
- [49] Sherly Abraham and InduShobha Chengalur-Smith. An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, 32(3):183–196, 2010.
- [50] Monique Bezuidenhout, Francois Mouton, and Hein S Venter. Social engineering attack detection model: Seadm. In *2010 Information Security for South Africa*, pages 1–8. IEEE, 2010.
- [51] Nabie Y Conteh and Paul J Schmick. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, 6(23):31, 2016.
- [52] Nabie Y Conteh and Malcolm D Royer. The rise in cybercrime and the dynamics of exploiting the human vulnerability factor. *International Journal of Computer (IJC)*, 20(1):1–12, 2016.
- [53] Xin Luo, Richard Brody, Alessandro Seazzu, and Stephen Burd. Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, 24(3):1–8, 2011.
- [54] Ping Chen, Lieven Desmet, and Christophe Huygens. A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security*, pages 63–72. Springer, 2014.
- [55] Radha Gulati. The threat of social engineering and your defense against it. *SANS Reading Room*, 2003.
- [56] Mercy Bere, Fungai Bhunu-Shava, Attlee Gamundani, and Isaac Nhamu. How advanced persistent threats exploit humans. *International Journal of Computer Science Issues (IJCSI)*, 12(6):170, 2015.
- [57] Adam Barth, Juan Caballero, and Dawn Song. Secure content sniffing for web browsers, or how to stop papers from reviewing themselves. In *2009 30th IEEE Symposium on Security and Privacy*, pages 360–371. IEEE, 2009.